Class Activity: RSA Encryption and Decryption

Instructions for Team A

(that wants to receive a secure message from Team B)

Part A1: Choose $\boldsymbol{p, q}$, then compute $\boldsymbol{n, e, d}$

Let $p = 3$ and $q = 23$

Compute $n = pq$. Result: $n =$ ________

Compute $(p-1)(q-1)$. Result: $(p-1)(q-1) =$ ______________

Let $e = 9$.

Compute a positive multiplicative inverse for e modulo $(p-1)(q-1)$. Call the inverse d.

Result: $d =$ multiplicative inverse for e mod $(p-1)(q-1) =$ ____________

Part A2: Send Team B the values of $\boldsymbol{n}$ and $\boldsymbol{e}$. (Do not send them the values of $\boldsymbol{p, q, d}$!!)

(Sit back and relax for awhile.)

Part A3: Receive the list of numbers $\boldsymbol{C_1, C_2, \ldots, C_k}$ from Team B

The list of numbers is:

____

Part A4: Compute Numbers $\boldsymbol{M_1, M_2, \ldots M_k}$

For each number C_j, compute the corresponding number

$$M_j = \left(C_j\right)^d \bmod n$$

(Use Wolfram Alpha for these calculations!)

Check: Each M_j should be in the range 1 – 26.

The result is the list of numbers:

____

Part A5: Find the corresponding letters $\boldsymbol{\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_k}$

Convert each of the numbers $M_1, M_2, \ldots, M_k$ (each in the range 1 – 26) into a letter $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_k$ from a to z.

The result is the list of letters:

____

The word is

____

Class Activity: RSA Encryption and Decryption

Instructions for Team B

(that is being asked to send a secure message to Team A)

Part B1: Choose a word $\mathcal{L}_1\mathcal{L}_2 \ldots \mathcal{L}_k$ that you want to send to Team A.

The word that you want to send to Team A is:

____

Part B1: For the word that you want to send to Team A, convert each of the letters $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_k$ into a number $M_1, M_2, \ldots, M_k$ from 1 – 26.

The result is the list of numbers:

____

Part B2: Receive the Public Key $n =$ _____ and $e =$ ____ from Team A

Part B3: Compute Numbers $C_1, C_2, \ldots, C_k$

For each number M_j, compute corresponding number

$$C_j = \left(M_j\right)^e \bmod n$$

(Use Wolfram Alpha for these calculations!)

The result is the list of numbers:

____

Part B4: Send the list of numbers $C_1, C_2, \ldots, C_k$ to Team A